

# TRANSVERSALS AS GENERATING SETS IN FINITELY GENERATED GROUPS

JACK BUTTON, MAURICE CHIODO, MARIANO ZERON-MEDINA LARIS

**ABSTRACT.** We explore transversals of finite index subgroups of finitely generated groups. We show that when  $H$  is a subgroup of a rank  $n$  group  $G$  and  $H$  has index at least  $n$  in  $G$  then we can construct a left transversal for  $H$  which contains a generating set of size  $n$  for  $G$ , and that the construction is algorithmic when  $G$  is finitely presented. We also show that, in the case where  $G$  has rank  $n \leq 3$ , there is a simultaneous left-right transversal for  $H$  which contains a generating set of size  $n$  for  $G$ . We finish by showing that if  $H$  is a subgroup of a rank  $n$  group  $G$  with index less than  $n + 2^n$ , and  $H$  contains no primitive elements of  $G$ , then  $H$  is normal in  $G$  and  $G/H \cong C_2^n$ .

## 1. INTRODUCTION

Let  $H$  be a subgroup of  $G$  (written  $H < G$ ). A *left transversal* for  $H$  in  $G$  is a choice of exactly one representative from each left coset of  $H$ . A *right transversal* for  $H$  in  $G$  is defined in an analogous fashion. A *left-right transversal* for  $H$  in  $G$  is a set  $S$  which is simultaneously a left transversal, and a right transversal, for  $H$  in  $G$ . The existence of a left or right transversal is clear (assuming the Axiom of Choice) whereas it is not immediate that a left-right transversal always exists. We gave a short proof of this in [3] for the case where  $H$  is of finite index, as well as a brief historical discussion of this result.

Transversals are natural objects of study, especially when  $H$  has finite index in  $G$ . Moreover, finding generating sets for a group  $G$  is a well known problem in the case when  $G$  is finitely generated. Therefore we can ask: given a finitely generated group  $G$  and a finite index subgroup  $H$  of  $G$ , is there a (say) left transversal for  $H$  in  $G$  which also generates  $G$ ? (In fact if  $T$  is a left transversal for  $H$  in  $G$ , then it is clear that  $T^{-1}$  (the set of inverses of all elements in  $T$ ) is a right transversal of  $H$  in  $G$ . Moreover  $\langle S \rangle = \langle S^{-1} \rangle$  for any subset  $S$  of a group  $G$ , so we need only consider left transversals throughout.) Jain asked Cameron this question under the added assumption that  $G$  is a finite group and  $H$  is corefree in  $G$ , meaning that  $\text{core}_G(H) = \{e\}$  ( $\text{core}_G(H)$  is the intersection of all conjugates of  $H$  in  $G$ :  $\text{core}_G(H) := \bigcap_{g \in G} g^{-1}Hg$ ). Cameron showed in [4] that in this case a generating left transversal always exists (see also [5, Problem 100]).

---

2010 *AMS Classification*: 20E99, 20F05

*Keywords*: Transversals, generating sets, finite index subgroups, primitive elements.

The second author was partially funded by the Italian FIRB “Futuro in Ricerca” project RBFR10DGUA.002 and the Swiss National Science Foundation grant FN PP00P2-144681/1.

The third author did part of this work while writing his thesis at the University of Cambridge, supported by the Mexican National Council for Science and Technology.

*Date*: February 5, 2014.

The proof is short but relies on a result [17] of Whiston on *minimal* generating sets (ones where no proper subset generates) of the symmetric group which uses the classification of finite simple groups (CFSG).

However there is an obvious necessary condition for a subgroup  $H$  of  $G$  to possess a generating left transversal, which is that the index  $[G : H]$  must be at least  $d(G)$  (the *rank* of  $G$ ), defined to be the minimal number of generators for the finitely generated group  $G$ . We show that this condition is also sufficient in Theorem 3.9 for  $G$  any finitely generated group and  $H$  any subgroup of finite index. We can then try to strengthen this result by examining whether  $[G : H] \geq d(G)$  implies that there exists a left-right transversal for  $H$  that generates  $G$ . We have not managed to establish this in general but we have shown in Theorem 3.14 that it is true if  $d(G) \leq 3$ . Moreover, in Section 4 we give sufficient additional conditions for our techniques from Section 3 to be algorithmic.

An element of a rank  $n$  group  $G$  is *primitive* if it lies in some generating set of size  $n$  for  $G$ . The location of primitive elements relative to cosets of subgroups is already an area of interest. Parzanchevski and Puder [16] show that if  $w \in F_n$  is a non-primitive element then there is a finite index subgroup  $H < F_n$  such that the coset  $wH$  does not contain any primitive elements. Taking  $w = e$  gives a finite index subgroup containing no primitive elements.

By applying some of the technique of *shifting boxes* developed in Section 3, we are able to show in Theorem 5.5 that if  $G$  is a rank  $n$  group, then the only subgroup of  $G$  with index less than  $n + 2^n$  that can contain *no* primitive elements is  $[G, G]G^2$ , and even then this only occurs when  $G/([G, G]G^2) \cong C_2^n$ . This gives an exponential lower bound on the index of subgroups which contain no primitive elements.

With  $N$  a normal subgroup of a finitely generated group  $G$ , we show in Proposition 5.6 that if  $N$  contains a primitive element then so do all cosets of  $N$ . Moreover, in Theorem 5.9 we see that if  $H$  is a subgroup of a rank  $n$  group  $G$  with  $[G : H] \leq n + 2$  then, except for the single case where  $n = 2$  and  $H = [G, G]G^2$  with  $G/H \cong C_2^2$ , all cosets of  $H$  contain a primitive element.

We first announced many of the results of this paper in [2].

**Acknowledgements:** We wish to thank Rishi Vyas and Andrew Glass for their many useful conversations and comments about this work. Thanks also go to Zachiri McKenzie and Philipp Kleppmann for discussions on the Axiom of Choice.

## 2. COSET INTERSECTION GRAPHS

A useful tool for studying the way left and right cosets interact, and obtaining transversals, is the coset intersection graph. In this section we re-state important results from our earlier work [3] on this concept.

**Definition 2.1.** Let  $H, K < G$ . We define the *coset intersection graph*  $\Gamma_{H,K}^G$  to be a graph with vertex set consisting of all left cosets of  $H$  ( $\{l_i H\}_{i \in I}$ ) together with all right cosets of  $K$  ( $\{Kr_j\}_{j \in J}$ ), where  $I, J$  are index sets. If a left coset of  $H$  and right coset of  $K$  correspond, they are still included twice. Edges

(undirected) are included whenever any two of these cosets intersect, and an edge between  $aH$  and  $Kb$  (written  $aH - Kb$ ) corresponds to the non-empty set  $aH \cap Kb$ .

**Theorem 2.2.**  $\Gamma_{H,K}^G$  is a disjoint union of complete bipartite graphs.

We denote the complete bipartite graph on  $(m, n)$  vertices by  $\mathbf{K}_{m,n}$ .

**Theorem 2.3.** Let  $H, K < G$ . Suppose that  $[G : H] = n$ ,  $[G : K] = m$ . Then the graph  $\Gamma_{H,K}^G$  is a collection of disjoint, finite, complete bipartite graphs, where each component is of the form  $\mathbf{K}_{s_i, t_i}$  with  $s_i/t_i = n/m$ .

**Corollary 2.4.** Let  $H, K < G$ . Suppose that  $[G : H] = n$  and  $[G : K] = m$ , where  $m \geq n$ . Then there exists a set  $T \subseteq G$  which is a left transversal for  $H$  in  $G$ , and which can be extended to a right transversal for  $K$  in  $G$ . If  $H = K$  in  $G$ , then  $T$  becomes a left-right transversal for  $H$ .

Under the hypothesis of Theorem 2.3, we see that sets of  $s_i$  left cosets of  $H$  completely intersect sets of  $t_i$  right cosets of  $K$ , with  $s_i/t_i$  constant over  $i$ . With this in mind, another way of visualising  $\Gamma_{H,K}^G$  is by the following simultaneous double-partitioning  $G$ : draw left cosets of  $H$  as columns, and right cosets of  $K$  as rows, partitioning  $G$  into irregular ‘chessboards’ denoted  $C_i$ , each with edge ratio  $n : m$ . Each chessboard  $C_i$  corresponds to the connected component  $\mathbf{K}_{s_i, t_i}$  of  $\Gamma_{H,K}^G$ , and individual tiles in  $C_i$  correspond to the non-empty intersection of a left coset of  $H$  and a right coset of  $K$  (i.e., edges in  $\mathbf{K}_{s_i, t_i}$ ). Corollary 2.4 would then follow by choosing one element from each tile on the leading diagonals of the  $C_i$ ’s. An example of chessboards is given in [3].

The chessboard pictorial representation of partitioning  $G$  into left and right cosets is extremely useful in the analysis of transversals as generating sets carried out in the next section. Note that the union of all the elements of  $G$  in a single chessboard gives a unique double coset  $KgH$  in  $G$ , and that a single chessboard is simply a double-partitioning of a double coset  $KgH$  into its respective left cosets of  $H$  and right cosets of  $K$ .

### 3. TRANSVERSALS AS GENERATING SETS

We have developed a technique which we call *shifting boxes* that, for the sake of brevity, we will describe here as a systematic way to apply Nielsen transformations to a generating set of a group  $G$ , such that the resulting generators lie inside (or outside) particular desired cosets of a subgroup  $H < G$ . We can’t ‘shift’ generators in/out of any coset we like, but we do have a substantial degree of control. For ease of notation, we will often refer to the coset  $eH$  as the *identity coset*. We begin with the following definitions.

**Definition 3.1.** Let  $G$  be a group, and  $S := (g_1, \dots, g_n)$  a generating  $n$ -tuple of  $G$  (where  $n \in \mathbb{N}$ ), that is, an element of the direct product  $G^n$  such that  $\{g_1, \dots, g_n\}$  generates  $G$ . A *standard Nielsen move* on  $S$  is the replacement of some entry  $g_i$  of  $S$  with one of  $g_j g_i, g_j^{-1} g_i, g_i g_j$  or  $g_i g_j^{-1}$ , where we must have  $i \neq j$ . A *Nielsen move* is defined to be either a standard Nielsen move or an *extended Nielsen move*, where the latter consists of either replacing an entry

$g_i$  by its inverse, or transposing two entries  $g_i$  and  $g_j$  for  $i \neq j$ . Note that on applying any Nielsen move to  $S$ , the resulting  $n$ -tuple still generates.

**Definition 3.2.** Let  $G$  be a group. Two generating  $n$ -tuples  $S_1, S_2$  of  $G$  are said to be *Nielsen equivalent* if they differ by a finite number of Nielsen moves.

**Definition 3.3.** Let  $G$  be a group,  $H$  a subgroup of  $G$ , and  $S$  a generating  $n$ -tuple of  $G$ . We say a left coset  $gH$  is *full* (with respect to  $S$ ) if some entry of  $S$  lies in  $gH$ , otherwise we say  $gH$  is *empty* (with respect to  $S$ ). To save on notation, we will usually suppress the term ‘with respect to  $S$ ’ when there is no ambiguity.

In the introduction we mentioned that the Axiom of Choice was necessary to show that for every group  $G$  and every subgroup  $H < G$  there exists a left transversal for  $H$  in  $G$  (in fact, the Axiom of Choice is equivalent to this condition; see [1, Theorem 2.1]). However, choice is *not* necessary for the groups we will be considering, as they are all finitely generated. To see this, take a finite generating set  $\{x_1, \dots, x_n\}$  for  $G$  and form the canonical enumeration of words  $w_1, w_2, \dots$  on  $X \cup X^{-1}$ , ordered lexicographically. Then the set  $T := \{w_n \in G \mid (\forall i < n)(w_i \notin w_n H)\}$  is a left transversal for  $H$  in  $G$  (and we have not used choice here). Moreover, if we have a set  $S \subset G$  for which no two elements of  $S$  lie in the same left coset of  $H$ , then this set extends to a left transversal for  $H$  by adjoining  $T_S := \{w_n \in G \mid (w_n \notin S) \wedge (\forall i < n)(w_i \notin w_n H)\}$  (again, without the need for choice).

We now give several techniques, which we rely on heavily for our main results. Note that in this section we prove our results under very general conditions, and all techniques are (for now) existential. Later, in Section 4, we give sufficient additional conditions for our techniques to be algorithmic.

**Lemma 3.4.** *Let  $G$  be a group,  $H$  a subgroup of  $G$ , and  $S$  a generating  $n$ -tuple of  $G$ . Then there is a generating  $n$ -tuple  $S'$  of  $G$ , Nielsen equivalent to  $S$ , such that no non-identity left coset of  $H$  contains more than one entry of  $S'$  (though  $eH$  may contain several entries). An identical result holds for right cosets of  $H$ .*

*Proof.* We call the following process *left-cleaning* an  $n$ -tuple. Let  $S = (g_1, \dots, g_n)$ . We can assume that there is  $g_i, g_j$  with  $i \neq j$  both lying in the same non-identity left coset of  $H$ , so that  $g_i H = g_j H \neq eH$ . Then  $g_j^{-1} g_i \in H$  so we can apply the standard Nielsen move on  $S$  which replaces  $g_i$  with  $g_j^{-1} g_i$  to obtain  $S_1$ . Then  $S_1$  has fewer entries lying in this left coset of  $H$ , and the same number in all other non-identity left cosets. Iterating this procedure and then moving to other non-identity left cosets, we eventually reach a set  $S'$  which only contains entries in distinct left cosets of  $H$  (apart from  $eH$  which may contain many entries of  $S'$ ). We say that a generating  $n$ -tuple possessing this property is a *left-cleaned*  $n$ -tuple.  $\square$

An analogous definition, result, and proof, applies for right cosets and right cleaning.

**Lemma 3.5.** *Let  $G$  be a group,  $H$  a subgroup of  $G$ , and  $S$  a generating  $n$ -tuple of  $G$ . If there exists at least one empty left coset of  $H$ , then there are*

entries  $s_j, s_k$  of  $S$  (possibly the same entry) and  $\epsilon \in \{\pm 1\}$  such that  $s_j^\epsilon s_k H$  is an empty left coset. That is, there is some full left coset of  $H$  which is taken to some empty left coset of  $H$  by left multiplication under some entry of  $S$  or its inverse.

*Proof.* Recall that  $G$  acts transitively on the set of left cosets by left multiplication. Assume that no entry of  $S$  or its inverse sends a full left coset to an empty left coset. Then, as the entries of  $S$  generate  $G$ , the collection of full left cosets is invariant under this action. Seeing as there exists at least one empty left coset, this contradicts the transitive action of  $G$ .  $\square$

**Lemma 3.6.** *Let  $G$  be a group,  $H$  a subgroup of  $G$ , and  $S$  a generating  $n$ -tuple of  $G$ . Suppose that at least one entry of  $S$  lies in  $H$ , and moreover that there exists an empty left coset of  $H$  with respect to  $S$ . Then there is a finite sequence of Nielsen moves on some entry  $s$  of  $S$  which is contained in  $H$  such that  $s$  is taken into an empty left coset of  $H$ .*

*Proof.* By Lemma 3.5 there are (possibly identical) entries  $s_1, s_2$  of  $S$ , and  $\epsilon \in \{\pm 1\}$ , with  $s_j^\epsilon s_k H$  an empty left coset of  $H$  with respect to  $S$ . We consider all possible cases:

1.  $s_j, s_k \in H$ .

This case never occurs, as then  $s_j^\epsilon s_k H = H$  which is a full left coset by hypothesis.

2.  $s_j \notin H, s_k \in H$ .

The subcase  $s_j^{+1} s_k H$  can't occur, as then  $s_j^{+1} s_k H = s_k^{+1} H$  which is clearly full. In the subcase  $s_j^{-1} s_k H$ , we replace  $s_k$  with  $s_j^{-1} s_k$  lying in the left coset  $s_j^{-1} s_k H$  which is empty.

3.  $s_j \in H, s_k \notin H$ .

In this case, we replace  $s_j$  with  $s_j^\epsilon s_k$ , as the left coset  $s_j^\epsilon s_k H$  is empty.

4.  $s_j, s_k \notin H$ .

In this case, take some  $s_i \in H$  and replace  $s_i$  with  $s_j^\epsilon s_k s_i$ , which lies in the empty left coset  $s_j^\epsilon s_k s_i H = s_j^\epsilon s_k H$ . As  $s_i$  is a different entry from  $s_j$  and  $s_k$ , this is a composition of two standard Nielsen moves on the entry  $s_i$  (even if  $s_j = s_k$ ).

We call this replacement process a *left-extraction* of an entry of  $S$  from  $H$ .  $\square$

**Lemma 3.7.** *Let  $G$  be a group,  $H$  a subgroup of  $G$ , and  $S$  a generating  $n$ -tuple of  $G$ . If  $n \leq [G : H]$  (allowing the possibility that  $[G : H] = \infty$ ), then there is an  $n$ -tuple  $S'$  Nielsen-equivalent to  $S$  such that no two entries of  $S'$  lie in the same left coset of  $H$ .*

*Proof.* Lemma 3.4 produces an  $n$ -tuple  $S''$  Nielsen-equivalent to  $S$  which is left-cleaned. Now repeatedly apply Lemma 3.6 to begin left-extracting elements from inside  $H$  (thus Nielsen-transforming  $S''$ ). As  $n \leq [G : H]$ , we can keep left-extracting until we reach  $S'$  which is Nielsen-equivalent to our original  $S$ , and for which no two entries of  $S'$  lie in the same left coset of  $H$ .  $\square$

For simplicity, when  $S$  is an  $n$ -tuple, we write  $\tilde{S}$  for the set of entries of  $S$ .

**Theorem 3.8.** *Let  $G$  be a group,  $S$  a generating  $n$ -tuple of  $G$ , and  $H < G$  a subgroup with  $n \leq [G : H]$  (allowing the possibility that  $[G : H] = \infty$ ). Then*

there is an  $n$ -tuple  $S'$  Nielsen-equivalent to  $S$ , and an extension  $T$  of  $\tilde{S}'$  such that  $T$  is a left transversal for  $H$  in  $G$ .

*Proof.* Take the generating  $n$ -tuple  $S$  of  $G$ . Use Lemma 3.7 to get a Nielsen-equivalent  $n$ -tuple  $S'$  for which no two entries lie in the same left coset of  $H$ . Now simply choose one element from each left coset of  $H$  which is empty with respect to  $S'$ , and add these to  $\tilde{S}'$  to form the set  $T$ . Then  $T$  is clearly a left transversal for  $H$ , and contains  $\tilde{S}'$ .  $\square$

Using these techniques, we state the condition below for a finite index subgroup of a group to possess a left transversal which generates the whole group.

**Theorem 3.9.** *Let  $G$  be a finitely generated group, and  $H$  a subgroup of finite index in  $G$ . Then the following are equivalent:*

1. *There exists a left transversal  $T$  for  $H$  in  $G$  with  $\langle T \rangle = G$ .*
2.  *$[G : H] \geq d(G)$ .*

As mentioned in the introduction, the above result also carries over to right transversals.

*Proof.* That  $1 \Rightarrow 2$  is immediate. To show  $2 \Rightarrow 1$ , take a generating  $n$ -tuple  $S$  of  $G$  with  $n = d(G)$  and apply Theorem 3.8.  $\square$

For ease of writing, we will often refer to the overall process of cleaning and/or extracting elements (either left, or right) as *shifting boxes*, and will usually just write *this follows by shifting boxes* to mean that it follows by the process of cleaning and/or extracting elements. Our remarks in this section give sufficient conditions for cleaning and/or extracting to be algorithmic.

The most natural question to ask now is ‘When does a finite index subgroup have a left-right transversal which generates the whole group?’ This requires a deeper understanding of how cosets intersect, as discussed in Section 2. We urge the reader to consider the discussion of ‘chessboards’ given after Corollary 2.4, and to consult [3] for an example. These are vital in proving the following results.

**Lemma 3.10.** *Let  $G$  be a group,  $H$  a subgroup of  $G$ , and  $S$  a generating  $n$ -tuple of  $G$ . Then by Lemma 3.4 we can first perform a left-cleaning of  $S$  to form  $S'$ , followed by a right-cleaning of  $S'$  (which will stay left-cleaned) to obtain a further generating  $n$ -tuple  $S''$  such that:*

1.  *$S$  and  $S''$  are Nielsen-equivalent.*
2.  *$S''$  is left-cleaned.*
3.  *$S''$  is right-cleaned.*

*We say that  $S''$  is left-right-cleaned.*

**Lemma 3.11.** *Let  $G$  be a group,  $H$  a subgroup of finite index in  $G$ , and  $S$  a generating  $n$ -tuple of  $G$ . Then  $S$  is left-right-cleaned if and only if one can draw chessboards for  $H$  in  $G$  with distinct entries of  $S$  lying in distinct diagonal tiles of chessboards, except for the chessboard corresponding to the double coset  $HeH = H$  which may contain several elements of  $S$ .*

*Proof.* This is immediate from the fact that columns in chessboards correspond to left cosets of  $H$ , and rows correspond to right cosets. Thus, a column (resp. row) in the chessboards contains multiple entries of  $S$  if and only if the corresponding left (resp. right) coset of  $H$  contains multiple entries of  $S$ .  $\square$

Note that one can obtain a left-right transversal for  $H$  by taking one element from each diagonal tile of each chessboard (by Corollary 2.4). More strongly, by left-right-cleaning and choosing an element from each unused diagonal we have:

**Lemma 3.12.** *Let  $G$  be a group,  $H$  a subgroup of finite index in  $G$ , and  $S$  a generating  $n$ -tuple of  $G$ . If  $S$  is left-right-cleaned, and  $H$  contains at most one entry of  $S$ , then there is a set  $T$  containing all the entries of  $S$  which is a left-right transversal for  $H$  in  $G$ .*

*Proof.* Given that that columns in chessboards correspond to left cosets of  $H$ , and rows correspond to right cosets, we have that no column or row in any chessboard contains more than one entry from  $S$ . Thus we can re-arrange the positioning of the columns and rows in each chessboard so that the entries of  $S$  are all in tiles which lie on leading diagonals. Now simply choose one element from each lead-diagonal tile which does not contain an entry of  $S$ , and add these to the set  $S$  to form the set  $T$ . Then  $T$  contains precisely one element from each lead-diagonal tile of each chessboard, and no other elements. Thus  $T$  contains precisely one element in each left coset of  $H$ , and precisely one element in each right coset of  $H$ . So  $T$  is our desired left-right transversal which contains  $\tilde{S}$ .  $\square$

Combining our shifting boxes technique, along with the properties of the coset intersection graph from Theorem 2.3, we are able to show the following:

**Theorem 3.13.** *Let  $G$  be a group,  $S$  a generating  $n$ -tuple for  $G$  with  $n \leq 3$ , and  $H$  a subgroup of finite index in  $G$  with  $n \leq [G:H]$ . Then there is a generating  $n$ -tuple  $S'$  Nielsen-equivalent to  $S$ , and a left-right transversal  $T$  for  $H$  in  $G$  with  $\tilde{S}' \subseteq T$ .*

*Proof.* The case when  $n = 1$  is trivial.

The case when  $n = 2$  is done as follows:

Left-right-clean  $S$  to form  $S' = (a, b)$ . Clearly we can't have  $a, b \in H$ , or else  $H$  can't have index  $\geq 2$ . So at most one of  $a, b$  lies inside  $H$ . But then by Lemma 3.12 we can extend  $\tilde{S}'$  to a set  $T$  which is a left-right transversal for  $H$ . Seeing as  $T$  contains  $\tilde{S}'$ , then it generates  $G$ .

The case where  $n = 3$  is much more complicated, and we need to consider several sub-cases. So, left-right-clean  $S$  to form  $S' = (a, b, c)$ . Clearly we cannot have  $a, b, c \in H$ , or else  $H$  does not have index at least 3. So at most two of  $a, b$  lie inside  $H$ . Again, if only one of  $a, b, c$  lies inside  $H$  then we can apply Lemma 3.12 as before. So we are left to consider what happens when two of  $a, b, c \in H$  (without loss of generality, re-label them as  $h_1, h_2 \in H$  and  $g \notin H$ ).

Case 1.  $g^2 \notin HgH \cup H$  (i.e.,  $g^2$  lies in a different chessboard to  $g$  and  $h_1, h_2$ ). Make the Nielsen moves  $h_1 \mapsto g^2 h_1$ ; this clearly lies in the same left coset (and hence same chessboard) as  $g^2$  (see Figure 1).

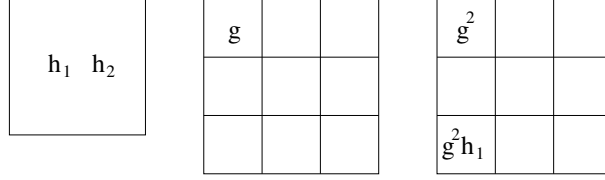


FIGURE 1.

So now each of  $g, h_2, g^2 h_1$  lie in different chessboards, thus the triple  $S'' := (g, h_2, g^2 h_1)$  is left-right cleaned. As only  $h_2$  lies inside  $H$ , we can use Lemma 3.12 to extend  $\tilde{S}''$  to a set  $T$  which is a left-right transversal for  $H$ . Seeing as  $T$  contains  $\tilde{S}''$ , then it generates  $G$ .

If case 1 does not occur, then we proceed to case 2.

Case 2.  $g^2 \in HgH$  (i.e.,  $g^2$  lies in the same chessboard as  $g$ ). Clearly  $g^2 H \neq gH$  and  $Hg^2 \neq Hg$ ; otherwise we would have  $g \in H$  which contradicts our initial hypothesis. So  $g^2$  lies in a different left coset and different right coset to  $g$  (i.e., in a different column and row to  $g$  in  $HgH$ ). Consider  $h_1 g^2$  and  $h_2 g^2$  (which both lie in the same right coset as  $g^2$ , and hence in a different right coset to  $g$ ). If  $h_i g^2 H \neq gH$  for some  $i \in \{1, 2\}$ , then make the Nielsen moves  $h_i \mapsto h_i g^2$  which lies in a different left and different right coset to  $g$  (but in the same chessboard) (see Figure 2).

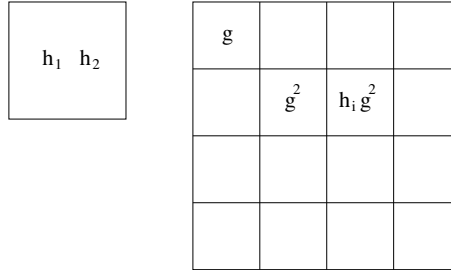


FIGURE 2.

If on the other hand  $h_1 g^2 H = h_2 g^2 H = gH$ , then  $h_2^{-1} h_1 g^2 H = g^2 H$  and so we make the Nielsen moves  $h_1 \mapsto h_2^{-1} h_1 g^2$  which lies in a different left and different right coset to  $g$  (but in the same chessboard) (see Figure 3).

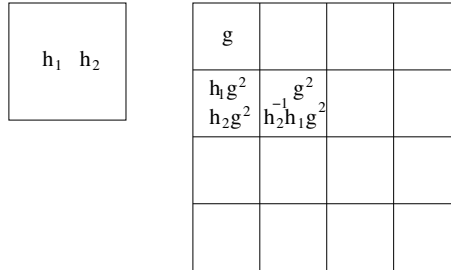


FIGURE 3.



Either way, we now have a triple  $S''$  for which, after permutation of some rows and columns, has entries which lie along diagonal tiles of the chessboards. As only one such entry lies inside  $H$ , we can use Lemma 3.12 to extend  $\tilde{S}''$  to a set  $T$  which is a left-right transversal for  $H$ . Seeing as  $T$  contains  $\tilde{S}''$ , then it generates  $G$ .

If neither case 1 nor case 2 occur, then we proceed to case 3.

Case 3.  $g^2 \in H$ .

By the transitivity of the action of  $G$  on left (and right) cosets of  $H$ , there must be some  $h_i$  ( $i \in \{1, 2\}$ ) and some  $\epsilon \in \{\pm 1\}$  with  $h_i^\epsilon gH \neq gH$ , and similarly some  $h_j$  ( $j \in \{1, 2\}$ ) and some  $\delta \in \{\pm 1\}$  with  $Hgh_j^\delta \neq Hg$ . If  $i \neq j$ , then we make the Nielsen move  $h_i \mapsto h_i^\epsilon g$  followed by the Nielsen move  $g \mapsto gh_j^\delta$  (see Figure 4).

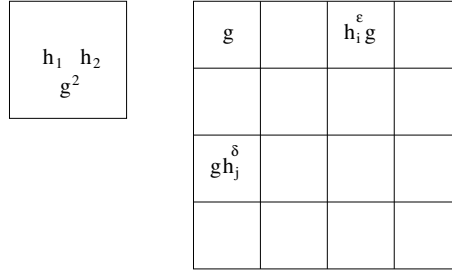


FIGURE 4.

If on the other hand  $i = j$  (say  $i = j = 1$ , without loss of generality), then consider the element  $h_2gh_1^\delta$ . If  $h_2gh_1^\delta H \neq gH$ , then  $h_2gh_1^\delta$  lies in a different left coset and different right coset to  $g$ , and so we make the Nielsen moves  $h_2 \mapsto h_2gh_1^\delta$  (see Figure 5).

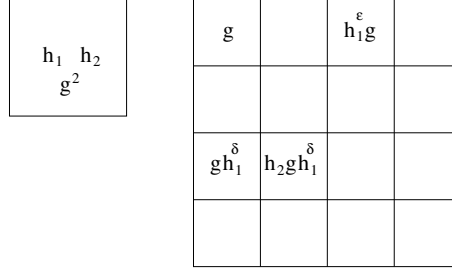


FIGURE 5.

If however  $h_2gh_1^\delta H = gH$ , then  $h_2gh_1^\delta$  lies in a different left coset and different right coset to  $h_1^\epsilon g$ , and so we make the Nielsen moves  $h_2 \mapsto h_2gh_1^\delta$  followed by  $g \mapsto h_1^\epsilon g$  (see Figure 6).

In all the subcases considered here, we end up with a triple  $S''$  for which, after permutation of some rows and columns, has entries which lie along diagonal tiles of the chessboards. As only one such entry lies inside  $H$ , we can use Lemma 3.12 to extend  $\tilde{S}''$  to a set  $T$  which is a left-right transversal for  $H$ . Seeing as  $T$  contains  $\tilde{S}''$ , then it generates  $G$ .  $\square$

$h_1 \ h_2$ $g^2$	$g$		$h_1^\varepsilon g$	
	$gh_1^\delta$ $h_2gh_1$			

FIGURE 6.

In the above proof, each case  $n = 1, 2, 3$  is shown by analysing a (increasing) finite number of possible scenarios, via repeated application of shifting boxes. We have not yet extended this to the case  $n \geq 4$ , as the number of scenarios to consider becomes very large and complex. We believe that the most elegant way to do this would be to establish some technique that, given a left-right-cleaned generating  $n$ -tuple  $S$  of  $G$  with more than one entry of  $S$  lying in  $H$ , left-right-extracts an entry of  $S$  lying in  $H$  to an empty square on the diagonal of one of the chessboards. We have not been able to do this, but believe that it may indeed be possible.

**Theorem 3.14.** *Let  $G$  be a group with  $d(G) \leq 3$ , and  $H$  a subgroup of finite index in  $G$ . Then the following are equivalent:*

1. *There exists a left-right transversal  $T$  for  $H$  in  $G$  with  $\langle T \rangle = G$ .*
2.  *$[G : H] \geq d(G)$ .*

*Proof.* That  $1 \Rightarrow 2$  is immediate. Conversely,  $2 \Rightarrow 1$  can be seen from Theorem 3.13.  $\square$

We note that, in any extension of Theorem 3.14 to groups needing more than three generators, we need only consider free groups, as the following shows:

**Proposition 3.15.** *Theorem 3.14 holds for all finitely rank groups (rather than just groups of rank at most 3) if and only if it holds for all finite rank free groups.*

*Proof.* Suppose Theorem 3.14 holds for all finite rank free groups. Let  $G$  be a group with  $d(G) = n$ , and  $H < G$  a subgroup of index  $[G : H] = k \geq n$ . Then there is a surjection  $f : F_n \twoheadrightarrow G$ , and it is a standard fact that the preimage  $f^{-1}(H)$  also has index  $k$  in  $F_n$ . By hypothesis, there is a left-right transversal  $T$  of  $f^{-1}(H)$  which generates  $F_n$ ; it follows that  $f(T)$  is a left-right transversal of  $H$  which generates  $G$ .  $\square$

Thus we are able to restrict our investigation to the case of finite rank free groups. By doing this, we are able to make use of the theory of Stallings graphs for subgroups of free groups [10]. This simplification to free groups also extends to all earlier results in this section before Theorem 3.14 (they are true for all groups if and only if they are true for free groups). With the help of Enric Ventura and Jordi Delgado we have found proofs to many of our earlier results using the framework of Stallings graphs. However, these are more

complicated, and attempts to generalise (or even re-prove) Theorem 3.14 using these techniques have so far been unsuccessful.

#### 4. ALGORITHMIC NATURE OF SHIFTING BOXES

In this section we revise most of the results from Section 3, and in each case give a set of sufficient conditions for the proof techniques used to be algorithmic, as well as describe these algorithms in full. We require some notation for this: If  $X$  is a set then we write  $X^*$  to denote the set of finite words on  $X \cup X^{-1}$ . A group presentation  $\langle X|R \rangle$  is said to be a *recursive presentation* if  $X$  is a finite set and  $R$  is a recursive enumeration of words in  $X^*$  (that is,  $R$  the halting set of some Turing machine on alphabet  $X \cup X^{-1}$ ).

For the remainder of this section, the symbol  $\mathfrak{G}$  will always denote a recursively presented group, and  $H$  will denote a finitely generated subgroup of  $\mathfrak{G}$ . When describing algorithms we will write “on input of  $\mathfrak{G}$  and  $H < \mathfrak{G}$ ” to mean “on input of a recursive presentation  $\langle X|R \rangle$  for the group  $\mathfrak{G}$ , and a finite set  $Y \subset X^*$  which generates the subgroup  $H < \mathfrak{G}$ ”.

**Proposition 4.1.** *There is an algorithm that, on input of  $\mathfrak{G}$  and  $H < \mathfrak{G}$  of finite index, the index  $[G : H]$ , and a solution to the subgroup membership problem for  $H$  in  $G$ :*

1. *Allows us to compute a left transversal  $T \subset X^*$  for  $H$  in  $\mathfrak{G}$ .*
2. *Given some word  $w \in X^*$ , allows us to compute some  $t_i \in T$  ( $T$  as above) such that  $w \in t_i H$ .*

*Proof.* The survey article [13] by Miller gives an excellent account of algorithmic processes in group theory such as these, so we omit their proofs here.  $\square$

**Proposition 4.2.** *There is an algorithm that, on input of a finite presentation  $\langle X|R \rangle$  of a group  $G$ , and a finite set  $Y$  which generates a subgroup  $H < G$  of finite index:*

1. *Allows us to compute the index  $[G : H]$ .*
2. *Allows us to solve the membership problem for  $H$  in  $G$ .*

*Hence we may also compute the objects mentioned in Proposition 4.1.*

*Proof.* This forms part of the Todd-Coxeter algorithm for enumerating finite index subgroups, first proved in [7]. We omit the proof here.  $\square$

**Proposition 4.3** (An algorithm for Lemma 3.4). *There exists an algorithm that, on input of  $\mathfrak{G}$  and  $H < \mathfrak{G}$ , an algorithm which solves the membership problem for  $H$  in  $\mathfrak{G}$ , and a generating  $n$ -tuple  $S$  for  $\mathfrak{G}$  (written with entries in  $X^*$ ); outputs a left-cleaned generating  $n$ -tuple  $S'$  for  $\mathfrak{G}$  which is Nielsen-equivalent to  $S$ , along with a sequence of Nielsen moves taking  $S$  to  $S'$ .*

*Proof.* Writing  $S$  as  $(s_1, \dots, s_n)$ , we use the solution to the membership problem for  $H$  to check if  $s_i^{-1}s_1 \in H$  for each  $i > 1$  in ascending order. If there is such an  $i$  with  $s_i^{-1}s_1 \in H$ , then at the first such instance  $i_1$ , replace  $s_1$  by  $s_{i_1}^{-1}s_1$  (a Nielsen move on  $S$ ). If no such  $i$  exists, then make no such replacement. Now start checking if  $s_i^{-1}s_2 \in H$  for each  $i > 2$  in ascending order, repeating the same procedure as for  $s_1$  above. Continue this for each entry  $s_3, \dots, s_n$  of  $S$ . The resulting  $n$ -tuple  $S'$  will be left-cleaned.  $\square$

From hereon we will refrain from explicitly stating that generating  $n$ -tuples are written with entries in  $X^*$ .

**Proposition 4.4** (An algorithm for Lemma 3.5). *There exists an algorithm that, on input of  $\mathfrak{G}$  and  $H < \mathfrak{G}$ , an algorithm which solves the membership problem for  $H$  in  $\mathfrak{G}$ , and a generating  $n$ -tuple  $S$  for  $\mathfrak{G}$  such that  $H$  has an empty left coset with respect to  $S$ ; outputs two (possibly identical) entries  $s_j, s_k$  of  $S$  and  $\epsilon \in \{\pm 1\}$  such that  $s_j^\epsilon s_k H$  is an empty left coset.*

*Proof.* For each triple of entries  $s_i, s_j, s_k$  in  $S$ , we can use the solution to the membership problem for  $H$  to check if  $s_i^{-1} s_j^{\pm 1} s_k \in H$ . By Lemma 3.5, we know that we will eventually find entries  $s_{j_1}, s_{k_1}$ , and  $\epsilon \in \{\pm 1\}$ , such that for all  $i$  we have  $s_i^{-1} s_{j_1}^\epsilon s_{k_1} \notin H$ . Thus  $s_{j_1}^\epsilon s_{k_1}$  lies in an empty left coset of  $H$ .  $\square$

**Proposition 4.5** (An algorithm for Lemma 3.6). *There exists an algorithm that, on input of  $\mathfrak{G}$  and  $H < \mathfrak{G}$ , an algorithm which solves the membership problem for  $H$  in  $\mathfrak{G}$ , and a generating  $n$ -tuple  $S$  for  $\mathfrak{G}$  such that at least one entry of  $S$  lies in  $H$  and moreover that there exists an empty left coset of  $H$  with respect to  $S$ ; outputs an entry  $s$  of  $S$  lying in  $H$  and a sequence of Nielsen moves taking  $s$  to some  $s'$  in an empty left coset of  $H$  with respect to  $S$ .*

*Proof.* Use Proposition 4.4 to generate entries  $s_j, s_k$  of  $S$  and  $\epsilon \in \{\pm 1\}$  such that  $s_j^\epsilon s_k H$  is an empty left coset. Now use the solution to the membership problem for  $H$  to decide precisely which case (1, 2, 3 or 4) occurs in the proof of Lemma 3.6, by deciding which of  $s_j, s_k$  lie in  $H$  if any, and construct the corresponding sequence of Nielsen moves as per the proof of Lemma 3.6.  $\square$

**Proposition 4.6** (An algorithm for Lemma 3.7). *There exists an algorithm that, on input of  $\mathfrak{G}$  and  $H < \mathfrak{G}$ , a generating  $n$ -tuple  $S$  for  $G$  with  $n \leq [G : H]$  (allowing the possibility that  $[G : H] = \infty$ ), and an algorithm which solves the membership problem for  $H$  in  $\mathfrak{G}$ ; outputs a generating  $n$ -tuple  $S'$  Nielsen-equivalent to  $S$ , along with a sequence of Nielsen moves taking  $S$  to  $S'$ , such that no two entries of  $S'$  lie in the same left coset of  $H$ .*

*Proof.* Use Proposition 4.3 to produce an  $n$ -tuple  $S''$  Nielsen-equivalent to  $S$  which is left-cleaned. Now repeatedly apply Proposition 4.5 to begin left-extracting elements from inside  $H$  (thus Nielsen-transforming  $S''$ ). As  $n \leq [G : H]$ , we can keep left-extracting until we reach  $S'$  which is Nielsen-equivalent to our original  $S$  and for which no two entries of  $S'$  lie in the same left coset of  $H$ .  $\square$

**Proposition 4.7** (An algorithm for Theorem 3.8). *There exists an algorithm that, on input of  $\mathfrak{G}$  and  $H < \mathfrak{G}$  of finite index, a generating  $n$ -tuple  $S$  for  $\mathfrak{G}$  with  $n \leq [\mathfrak{G} : H]$ , the index  $[\mathfrak{G} : H]$ , and an algorithm which solves the membership problem for  $H$  in  $\mathfrak{G}$ ; outputs an  $n$ -tuple  $S'$  Nielsen-equivalent to  $S$ , a sequence of Nielsen moves from  $S$  to  $S'$ , and a finite set  $T'$  which is a left transversal for  $H$  and contains  $\tilde{S}'$ .*

*Proof.* Take the generating  $n$ -tuple  $S$  of  $\mathfrak{G}$ . Use Proposition 4.6 to construct a Nielsen-equivalent  $n$ -tuple  $S'$  for which no two entries lie in the same left coset of  $H$  (along with the corresponding sequence of Nielsen moves). Now use

Proposition 4.1 to construct a left transversal  $T$  for  $H$ . As no two entries of  $S'$  lie in the same left coset of  $H$ , we can use Proposition 4.1 again to find, for each entry  $s'_i$  in  $S'$ , a corresponding element  $t_{j_i}$  in  $T$  for which  $s'_i \in t_{j_i}H$ . Now form the finite set  $T'$  by replacing each  $t_{j_i}$  with  $s'_i$  for each entry  $s'_i$  in  $S'$ . By construction,  $T'$  is a left transversal for  $H$ , and contains  $\tilde{S}'$ .  $\square$

**Proposition 4.8** (An algorithm for Lemma 3.10). *There exists an algorithm that, on input of  $\mathfrak{G}$  and  $H < \mathfrak{G}$ , an algorithm which solves the membership problem for  $H$  in  $\mathfrak{G}$ , and a generating  $n$ -tuple  $S$  for  $G$ ; outputs a left-right-cleaned generating  $n$ -tuple  $S'$  Nielsen-equivalent to  $S$ , along with a sequence of Nielsen moves taking  $S$  to  $S''$ .*

*Proof.* Use Proposition 3.4 to form a left-cleaned  $n$ -tuple  $S'$  Nielsen-equivalent to  $S$ , and again to form a right-cleaned  $n$ -tuple  $S''$  Nielsen-equivalent to  $S'$  (which will remain left cleaned). Each application of Proposition 3.4 produces a corresponding sequence of Nielsen moves.  $\square$

**Proposition 4.9** (An algorithm for Lemma 3.12). *There exists an algorithm that, on input of  $\mathfrak{G}$  and  $H < \mathfrak{G}$  of finite index, the index  $[\mathfrak{G} : H]$ , an algorithm which solves the membership problem for  $H$  in  $\mathfrak{G}$ , and a generating  $n$ -tuple  $S$  for  $\mathfrak{G}$  with  $n \leq [\mathfrak{G} : H]$  which is left-right-cleaned and for which at most one entry of  $S$  is contained in  $H$ ; outputs a left-right transversal  $T'$  for  $H$  in  $\mathfrak{G}$  with  $\tilde{S} \subseteq T'$ .*

*Proof.* Using Proposition 4.1, we can construct a left transversal  $T$  for  $H$ . As  $T$  is a left transversal, then  $T^{-1}$  is a right transversal. So we can use the solution to the membership problem for  $H$  to draw the chessboards for  $H$  in  $\mathfrak{G}$  and to locate each entry  $s_i$  of  $S$  in its corresponding row and column (that is, its corresponding left and right transversal of  $H$ ). As  $S$  is left-right-cleaned, we can re-order the rows and columns of the chessboards so that distinct entries of  $S$  lie in distinct diagonal tiles of chessboards (by Lemma 3.11). Now, for each empty diagonal tile (which corresponds to the intersection  $t_k H \cap H t_l^{-1}$  for some  $t_k, t_l \in T$ ), we can use the solution to the membership problem for  $H$  to find an element in this intersection. The union of these new elements, along with the entries of  $S$ , form a left-right transversal  $T'$  of  $H$  in  $\mathfrak{G}$ .  $\square$

**Proposition 4.10** (An algorithm for Theorem 3.13). *There exists an algorithm that, on input of  $\mathfrak{G}$  and  $H < \mathfrak{G}$  of finite index, the index  $[\mathfrak{G} : H]$ , an algorithm which solves the membership problem for  $H$  in  $\mathfrak{G}$ , and a generating  $n$ -tuple  $S$  for  $\mathfrak{G}$  with  $n \leq 3$  and  $n \leq [\mathfrak{G} : H]$ ; outputs a generating  $n$ -tuple  $S'$  Nielsen-equivalent to  $S$ , a sequence of Nielsen moves taking  $S$  to  $S'$ , and a left-right transversal  $T'$  for  $H$  in  $\mathfrak{G}$  with  $\tilde{S}' \subseteq T'$ .*

*Proof.* We can use the solution to the membership problem for  $H$  to show that all the steps in the proof of Theorem 3.13 are algorithmic, and thus we can construct a generating  $n$ -tuple  $S'$  Nielsen-equivalent to  $S$  for which no two entries lie in the same left or right coset of  $H$  (to re-write this would be somewhat arduous, so we encourage the reader to go through the proof of Theorem 3.13 and verify each step). Now apply Proposition 4.9 to construct a left-right transversal  $T'$  which extends  $\tilde{S}'$ .  $\square$

Recall that, by Proposition 4.2, in the case that  $G$  is finitely presented and  $H$  is of finite index, all earlier remarks describe algorithms which are uniform on input of  $G$  (given by a finite presentation) and  $H$  (given by a finite generating set); there is no need to input an explicit algorithm for the subgroup membership problem for  $H$  in  $G$ , or for the index  $[G : H]$ , as these can both be computed directly.

## 5. AN APPLICATION OF SHIFTING BOXES: FINDING PRIMITIVE ELEMENTS

Recall that a primitive element of a finite rank free group  $F_n$  is one which lies in *some* generating set of size precisely  $n$ , which is equivalent to being an element of a free basis for  $F_n$ . If  $G$  is a group of finite rank  $n$ , then we say a *primitive element* in  $G$  is an element lying in *some* generating set of size  $n$  for  $G$ . This reduces to the standard definition of primitive elements in finitely generated free groups.

An obvious question to ask is which subgroups of  $F_n$  (or more generally, rank  $n$  groups) contain a primitive element (we can ask this for both finite and infinite index subgroups). We first consider the case of normal subgroups.

The following is immediate by considering the image under the natural homomorphism of a generating set of minimal size containing the relevant primitive element:

**Lemma 5.1.** *Let  $G$  be a group of finite rank, and  $N$  a normal subgroup of  $G$ . If  $N$  contains some primitive element of  $G$ , then  $d(G/N) < n$ .*

The converse statement is not true, even in the special case that  $G = F_n$ , as was shown in [14] and in [9] as well as in more recent work (though it is true if  $N$  is the normal closure of a single element by [11, §II Proposition 5.11]) but in all of these cases  $N$  has infinite index. It is currently open if  $N$  has finite index, as will be seen once we have introduced the connection with product replacement graphs. Our source for this topic is the survey article [15] of Pak which contains a range of references.

Given a finitely generated group  $G$  and an integer  $n \geq d(G)$ , the product replacement graph  $\Gamma_n(G)$  has vertices the generating  $n$ -tuples of  $G$  with edges between two vertices if one is the image of another under a standard Nielsen move. (As these moves are reversible, we take the graph to be undirected.) We also have the extended product replacement graph  $\tilde{\Gamma}_n(G)$  where we allow all Nielsen moves. One big area of study in this topic is the connectivity of  $\Gamma_n(G)$  and  $\tilde{\Gamma}_n(G)$ . Now if  $n \geq d(G) + \bar{d}(G)$ , where  $\bar{d}$  is the maximum size of a *minimal* generating set (one in which no proper subset is a generating set), then it is known that  $\Gamma_n(G)$  (and hence  $\tilde{\Gamma}_n(G)$ ) is connected. However  $\bar{d}$  can be a very hard quantity to evaluate in practice: indeed the result of Whiston mentioned earlier which was used by Cameron is that  $\bar{d}(S_n) = n - 1$  and the proof needed CFSG. Moreover  $\bar{d}(G)$  need not be finite for finitely generated groups which are infinite: for instance on taking  $G = \mathbb{Z}$  we can see that  $\Gamma_n(G)$  is connected for  $n > 1$  by the Euclidean algorithm, but  $G$  has finite generating sets which are minimal but of arbitrary size.

Indeed it is possible that  $\Gamma_n(G)$  and  $\tilde{\Gamma}_n(G)$  are disconnected when  $n = d(G)$ , as happens for most finite abelian groups. However no example is known of a finite group  $G$  and an integer  $n > d(G)$  where  $\Gamma_n(G)$  or  $\tilde{\Gamma}_n(G)$  is disconnected (in fact the two statements are equivalent when  $n > d(G)$ ). If  $G$  is finite soluble and  $n > d(G)$  then Dunwoody showed in [8] that  $\Gamma_n(G)$  is connected. The relation with primitive elements, as also noted by Dunwoody in that paper, is that if  $N$  is a normal subgroup of  $F_n$  containing no primitive element but  $G = F_n/N$  has  $d(G) < n$  then  $\Gamma_n(G)$  is disconnected. This follows by taking a free basis  $x_1, \dots, x_n$  for  $F_n$  which gives rise to a generating  $n$ -tuple  $(\pi(x_1), \dots, \pi(x_n))$  for  $G$ , where  $\pi$  is the natural homomorphism from  $F_n$  to  $G$ . However we can also extend the smaller generating set for  $G$  to a generating  $n$ -tuple  $(g_1, \dots, g_n) \in G^n$ . Now if we could get from the first  $n$ -tuple to the second by Nielsen moves then we can apply the same moves to  $(x_1, \dots, x_n)$ , resulting in a free basis  $(z_1, \dots, z_n)$  of  $F_n$  such that

$$(\pi(z_1), \dots, \pi(z_n)) = (g_1, \dots, g_n)$$

so  $N$  contains the primitive element  $z_n$ . Thus we conclude that if  $N$  contains no primitive element then  $\tilde{\Gamma}_n(G)$  and  $\Gamma_n(G)$  are disconnected. Hence there are examples of infinite finitely generated groups  $G$  with  $\Gamma_n(G)$  disconnected by the papers cited above, but a normal subgroup  $N$  of finite index containing no primitive element and with  $d(F_n/N) < n$  would give rise to a finite group  $G$  and integer  $n > d(G)$  with  $\Gamma_n(G)$  disconnected; it is currently unknown whether such a group exists or not.

Our shifting boxes technique enables us to explore the location of primitive elements relative to cosets of a finite index subgroups, in the following ways:

**Theorem 5.2.** *Let  $G$  be any group with  $d(G) = n$ , and  $H$  a subgroup of finite index in  $G$  with  $[G : H] < n + 2^n$ . Then at least one of the following occur:*

1.  *$H$  contains at least one primitive element of  $G$ .*
2.  *$H$  contains the square of every primitive element of  $G$ .*

*Proof.* Suppose that  $H$  contains no primitive element; we show that condition 2 of the theorem must hold. Recall that  $[G : H] < n + 2^n$ . Now, take any left-cleaned generating  $n$ -tuple  $S = (g_1, \dots, g_n)$  for  $G$  (if it were not left-cleaned then we would have a primitive element in  $H$  by left-cleaning, as in Lemma 3.4). Consider the following list of elements of  $G$  (partitioned for convenience):

- All  $n$  entries from  $S$ . i.e.,  $g_1, g_2, \dots, g_n$ .
- The trivial element. i.e.,  $e$ .
- All  $\binom{n}{1}$  ways of choosing 1 entry from  $S$ , followed by  $g_1$ . i.e.,  $g_1g_1, g_2g_1, \dots, g_ng_1$
- All  $\binom{n}{2}$  ways of choosing 2 entries from  $S$ , written in decreasing order, followed by  $g_1$ . i.e.,  
 $g_2g_1g_1, g_3g_1g_1, \dots, g_ng_1g_1$   
 $g_3g_2g_1, g_4g_2g_1, \dots, g_ng_2g_1$   
 $\vdots$   
 $g_ng_{n-1}g_1$
- $\vdots$

- All  $\binom{n}{n}$  ways of choosing  $n$  entries from  $S$ , written in decreasing order, followed by  $g_1$ . i.e.,  $g_n g_{n-1} \dots g_2 g_1 g_1$

Note that all choices of  $k$  entries from  $S$  are taken without repetition on indices. Thus the individual sets listed above have sizes  $n, \binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n}$  respectively. The following is then immediate from the construction of the above list: a) Apart from  $g_1 g_1$  and  $e$ , every element listed above is primitive (follows from the fact that all these other elements are a combination of Nielsen moves on one of the entries in  $S$ ).

b) If any two distinct elements in the above list (including  $g_1 g_1$  and  $e$ ) are in the same left coset of  $H$ , then either  $H$  contains a primitive element or  $g_1^2 \in H$ . The best way to see this is to consider what happens when an element in the list lies in the same coset as an element mentioned earlier in the list, and then progressively work through the list in this order. We give here an explicit analysis of all possible cases:

1.  $g_{i_1} \dots g_{i_k} g_1 H = g_{j_1} \dots g_{j_l} g_1 H$  with  $i_1 > \dots > i_k$  and  $j_1 > \dots > j_l$  (including the case that either of  $k, l$  are 0).

In this case, the element  $z := (g_{j_1} \dots g_{j_l} g_1)^{-1} g_{i_1} \dots g_{i_k} g_1$  lies in  $H$ , and is primitive as by construction there is some index  $t$  for which  $g_t^{\pm 1}$  appears only once in  $z$  and thus  $z$  can be obtained from  $g_t$  by Nielsen moves (With the following exception: if  $k = 1$ ,  $i_1 = 1$  and  $j = 0$  then  $z = g_1^{-1} g_1 g_1 = g_1$  which is primitive nonetheless).

2.  $g_{i_1} \dots g_{i_k} g_1 H = g_j H$  with  $i_1 > \dots > i_k$  (including the case  $k = 0$ ).

In this case, the element  $z := g_j^{-1} g_{i_1} \dots g_{i_k} g_1$  lies in  $H$ , and is primitive as by construction there is some index  $t$  for which  $g_t^{\pm 1}$  appears only once in  $z$  and thus  $z$  can be obtained from  $g_t$  by Nielsen moves (With the following exception: if  $k = 1$ ,  $i_1 = 1$  and  $j = 1$  then  $z = g_1^{-1} g_1 g_1 = g_1$  which is primitive nonetheless).

3.  $g_i H = g_j H$ .

In this case, the element  $z := g_j^{-1} g_i$  lies in  $H$  and is primitive.

4.  $g_{i_1} \dots g_{i_k} g_1 H = H$  with  $i_1 > \dots > i_k$  and  $k > 1$ .

In this case, the element  $z := g_{i_1} \dots g_{i_k} g_1$  lies in  $H$ , and is primitive as by construction there is some index  $t$  for which  $g_t^{\pm 1}$  appears only once in  $z$  and thus  $z$  can be obtained from  $g_t$  by Nielsen moves.

5.  $g_i g_1 H = H$ .

If  $i \neq 1$ , then the element  $z := g_i g_1$  is primitive and lies in  $H$ . If  $i = 1$  then the element  $g_1^2$  lies in  $H$ .

So, if we try to place all the elements above (including  $e$  and  $g_1 g_1$ ) into cosets, while simultaneously ensuring that  $H$  has no primitive element and that  $g_1^2 \notin H$ , we need at least this many cosets:

$$n + \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \dots + \binom{n}{n} = n + \sum_{i=0}^n \binom{n}{i} = n + 2^n$$

So, if  $H$  contains no primitive element, and  $[G : H] < n + 2^n$ , then  $g_1^2 \in H$ .

But now take *any* primitive element  $x \in G$ , and maintain that  $[G : H] < n + 2^n$ . Then  $x$  is part of some generating set  $\{x, y_2, \dots, y_n\}$  for  $G$ . Now run the exact same argument above, with  $g_1 := x$ ,  $g_i := y_i$  for all  $2 \leq i \leq n$ , and we see that if



$H$  contains no primitive element then  $x^2 \in H$ . Thus, if  $H$  contains no primitive element, and  $[G : H] < n + 2^n$ , then the square of *every* primitive element lies in  $H$ .  $\square$

We make the following useful observation.

**Lemma 5.3.** *Let  $G$  be a finitely generated group with  $d(G) = n$ , and  $H < G$  a subgroup of  $G$ . Then  $H$  contains the square of every primitive element of  $G$  if and only if  $H$  is normal in  $G$  and  $G/H \cong C_2^m$  for some  $m \leq n$ .*

*Proof.* Clearly, if  $H \triangleleft G$  and  $G/H \cong C_2^m$ , then  $H$  contains the square of every element of  $G$ . Conversely, suppose  $H$  contains the square of every element of  $G$ . Define the set  $T := \{g^2 \mid g \text{ is a primitive element of } G\}$ . Then  $T$  is a normal subset of  $G$ , since the conjugate of a primitive element is again a primitive element (conjugation is an automorphism). Thus  $\langle T \rangle \triangleleft G$ ; the (normal) subgroup generated by all the squares of primitive elements of  $G$ . So by hypothesis,  $T < H$ . Now take any generating set  $\{t_1, \dots, t_n\}$  for  $G$ , then  $t_i^{-1}t_j$  is a primitive element, for any pair  $i, j$  with  $i \neq j$ . Thus  $t_i^2, t_j^2, (t_i^{-1}t_j)^2$  lie in  $\langle T \rangle$ , and hence so will  $t_i^2(t_i^{-1}t_j)^2t_j^{-2} = [t_i, t_j]$ . So  $G/\langle T \rangle$  is abelian as  $\langle T \rangle$  is normal and contains the commutator of every pair in the generating set  $\{t_1, \dots, t_n\}$  for  $G$ . So  $\langle T \rangle$ , and hence  $H$ , contain the commutator subgroup  $[G, G]$ . Thus  $H$  is normal in  $G$  and  $G/H$  is generated by the images of  $\{t_1, \dots, t_n\}$ , all of which have order 2 in this quotient. So  $G/H \cong C_2^m$  for some  $m \leq n$ .  $\square$

We use Lemma 5.3 to reformulate Theorem 5.2 as follows:

**Theorem 5.4.** *Let  $G$  be any group with  $d(G) = n$ , and  $H$  a subgroup of finite index in  $G$  with  $[G : H] < n + 2^n$ . Then at least one of the following occur:*

1.  $H$  contains at least one primitive element of  $G$ .
2.  $H$  is normal in  $G$  and  $G/H \cong C_2^m$  for some  $m \leq n$ .

We now give the following complete characterisation of finite index subgroups of a group of rank  $n$  which contain primitive elements, up to index  $n + 2^n - 1$ .

**Theorem 5.5.** *Let  $G$  be any group with  $d(G) = n$  and let  $H$  be a subgroup of finite index in  $G$ , with  $[G : H] < n + 2^n$ . Then  $H$  contains no primitive elements of  $G$  if and only if  $H$  is normal in  $G$  and the quotient  $G/H$  is isomorphic to  $C_2^n$ , whereupon every coset distinct from  $H$  contains a primitive element of  $G$ .*

*Proof.* First if  $H$  is normal and contains an element  $g$  of a generating  $n$ -tuple for  $G$  then the image of this  $n$ -tuple gives rise to a generating  $(n - 1)$ -tuple of  $G/H$ , just as in Lemma 5.1, but  $d(C_2^n) = n$ .

Now suppose that  $H$  does not contain a primitive element of  $G$  and let  $q : G \rightarrow G/H$  be the quotient homomorphism, where we know  $H$  is normal in  $G$  and  $G/H \cong C_2^m$  for some  $m \leq n$  by Theorem 5.4. Given a generating  $n$ -tuple  $(g_1, \dots, g_n)$  for  $G$ , let  $F_n$  be the free group on  $x_1, \dots, x_n$  and set  $\theta : F_n \rightarrow G$  to be the homomorphism extending the map  $x_i \mapsto g_i$ . Note that if we have  $k \leq n$  and integers  $1 \leq i_1 < i_2 < \dots < i_k \leq n$  then  $x_{i_1}x_{i_2}\dots x_{i_k}$  is primitive in  $F_n$  and  $\theta(x_{i_1}x_{i_2}\dots x_{i_k}) = g_{i_1}g_{i_2}\dots g_{i_k}$  is primitive in  $G$ .

Assume that  $m < n$  and consider the map  $q \circ \theta : F_n \twoheadrightarrow C_2^m$ , which factors through  $C_2^n$  via the abelianisation map  $\text{ab} : F_n \twoheadrightarrow C_2^n$  and the map  $\psi : C_2^n \twoheadrightarrow C_2^m$ . That is, the following diagram commutes, and all maps are surjections:

$$\begin{array}{ccc} F_n & \xrightarrow{\text{ab}} & C_2^n \\ \theta \downarrow & & \downarrow \psi \\ G & \xrightarrow{q} & C_2^m \end{array}$$

As  $\psi$  is now a linear map from an  $n$  dimensional vector space over  $\mathbb{F}_2$  to an  $m$  dimensional space, we have a non-trivial element  $(v_1, \dots, v_n)$  of  $C_2^n$  in the kernel of  $\psi$ . Now we can assume that each  $v_i$  takes the value 0 or 1, so we form the primitive element  $x = x_1^{v_1} x_2^{v_2} \dots x_n^{v_n}$  of  $F_n$  which maps to the identity under  $\psi \circ \text{ab}$ , thus  $g_1^{v_1} g_2^{v_2} \dots g_n^{v_n} = \theta(x)$  is a primitive element of  $G$  which maps to the identity under  $q$  and so is in  $H$ ; a contradiction.

Similarly if  $n = m$  then, for any  $(w_1, \dots, w_n)$  in  $\mathbb{F}_2^n - \{0\}$ , the coset of  $H$  in  $G$  corresponding to this point contains the primitive element  $g_1^{w_1} g_2^{w_2} \dots g_n^{w_n}$  of  $G$ .  $\square$

Note that the inequality in the above theorem is somewhat necessary: here is an example of what occurs when the inequality doesn't hold.

**Example.** Take the standard quotient map  $f : F_n \twoheadrightarrow C_3^n$ , and define  $H := \ker(f)$ . Then  $H$  contains no primitive element by Lemma 5.1, and yet  $F_n/H \not\cong C_2^n$ . Note that  $[F_n : H] = 3^n \geq 2^n + n$ , so this is not a counterexample to Theorem 5.4.

Thus if  $G$  is a group with  $d(G) = n$  we have two possibilities: either  $C_2^n$  is not a quotient of  $G$  in which case all subgroups of  $G$  having index less than  $2^n + n$  contain primitive elements, or  $G$  surjects to  $C_2^n$  in which case there is a single subgroup of index less than  $2^n + n$  which fails to contain a primitive element. The uniqueness in the second case comes about because a homomorphism from a rank  $n$  group  $G$  to an abelian group of exponent 2 must factor through  $[G, G]G^2$ . As  $G/([G, G]G^2) \cong C_2^m$  for  $m \leq n$ , we see that when  $n = m$  any exceptional subgroup must be equal to  $[G, G]G^2$ .

In the case where  $G$  is equal to the free group  $F_n$ , we remark that the number of subgroups of  $F_n$  with index less than  $2^n + n$  is vast: for instance by [12, Corollary 2.1.2] the number of subgroups of  $F_n$  with index equal to  $2^n$  is bounded below by  $((2^n)!)^{n-1}$ , yet only one of these subgroups fails to contain a primitive element by Theorem 5.5. Even when  $G$  is abelian, this number can be superexponential: in the case of the free abelian group  $\mathbb{Z}^n$  we have a lower bound of  $2^{n^2-n-1}$  for the number of subgroups of index  $2^n$  by a straightforward argument in Proposition 1.5.1 of the same volume.

It would be interesting to find a closed form expression for  $M(n)$ , which we define to be the maximum integer  $i$  such that if  $H$  is a subgroup of  $F_n$  with index less than  $i$  then either  $H$  contains a primitive element or  $H = [F_n, F_n]F_n^2$ . We know that  $2^n + n \leq M(n) \leq 3^n$  by Theorem 5.5 and the example below it.

Let us now examine when every coset of a given subgroup of a rank  $n$  group  $G$  contains a primitive element. As usual we start by considering normal subgroups, where there is an obvious sufficient condition.

**Proposition 5.6.** *If  $G$  is a group with  $d(G) = n$  and  $N$  is a normal subgroup of  $G$  containing a primitive element of  $G$  then all cosets of  $N$  also contain a primitive element.*

*Proof.* Let  $(g_1, \dots, g_n)$  be a generating  $n$ -tuple for  $G$  and suppose without loss of generality that  $g_n \in N$ . Then for each non-identity element  $\gamma \in G/N$ , choose  $g \in G$  with  $\pi(g) = \gamma$  for  $\pi : G \rightarrow G/N$  the natural projection. Now we can express  $g$  as a word in  $g_1, \dots, g_n$  but we can remove all appearances of  $g_n$  from  $g$  to obtain an element  $g'$  of  $G$  which is expressed purely in terms of  $g_1, \dots, g_{n-1}$ . As  $g_n \in N$  we still have  $\pi(g') = \gamma$  and indeed  $\pi(g'g_n) = \gamma$ . But  $g'g_n$  is a primitive element in the coset  $g'N = \gamma$ .  $\square$

Thus we have the following corollary which follows immediately from this and Theorem 5.5.

**Corollary 5.7.** *Let  $G$  be any group with  $d(G) = n$ . If  $N$  is a normal subgroup of  $G$  having index less than  $2^n + n$  then all non-identity cosets of  $N$  contain a primitive element of  $G$ , as does  $N$  itself, apart from the one special exception where  $N = [G, G]G^2$  and  $G/N \cong C_2^n$ .*

Now we return to shifting boxes in order to consider primitive elements in cosets of non-normal subgroups.

**Lemma 5.8.** *Let  $n \geq 2$ ,  $d(G) \geq n$ , and  $H$  be a subgroup of  $G$  having index  $n+2$ . Then if  $S$  is a generating  $n$ -tuple of  $G$  for which no two entries of  $S$  lie in the same left coset and no entry of  $S$  lies in  $H$ , then every non-identity left coset of  $H$  contains a primitive element of  $G$ .*

*Proof.* Label the  $n$ -tuple  $S = (g_1, \dots, g_n)$ . By hypothesis, the two left cosets of  $H$  not containing entries of  $S$  are  $H$  and some  $xH$  ( $x \in G \setminus H$ ). Fix any entry  $g_i$  of  $S$ , and consider  $g_i xH$ . Then:

- a) We cannot have  $g_i xH = g_i H$ , as then  $xH = H$  contradicting our initial hypothesis that  $x \notin H$ .
- b) If  $g_i xH = g_j H$  for some  $i \neq j$ , then  $xH = g_i^{-1} g_j H$ , and so  $xH$  contains the primitive element  $g_i^{-1} g_j$ .
- c) If  $g_i xH = H$  then  $xH = g_i^{-1} H$ , so  $xH$  contains the primitive element  $g_i^{-1}$ .
- d) If  $g_i xH = xH$  then  $g_i$  stabilises  $xH$  under the left action of  $G$  on left cosets of  $H$ .

Assume  $xH$  contains no primitive elements. Then, for each  $g_i$ , case d) of the above list must occur (as  $g_i xH$  must be one of  $H, xH, g_1 H, \dots, g_n H$ ). Thus, each  $g_i$  stabilises  $xH$ , and so all of  $G$  stabilises  $xH$ . But this is a contradiction, as the action of  $G$  on left cosets of  $H$  is transitive and so no left coset is stabilised by all of  $G$ .  $\square$

**Theorem 5.9.** *Let  $G$  be any group with  $d(G) = n \geq 2$ . If  $H$  is a subgroup of  $G$  having index at most  $n+2$  then, except for the single case where  $n = 2$  and  $H = [G, G]G^2$  with  $G/H \cong C_2^2$ , every left (and hence every right) coset of  $H$  contains some primitive element of  $G$ .*

*Proof.* Take a generating  $n$ -tuple  $S$ . If any two entries of  $S$  lie in the same coset of  $H$  then we can use Lemma 3.4 to left-clean  $S$  to a Nielsen equivalent  $n$ -tuple  $S'$ . If now there are any empty left cosets of  $H$  with respect to  $S'$  then we can use Lemma 3.6 to begin left-extracting entries of  $S'$  from  $H$ , as we will have an entry of  $S'$  in  $H$ . We consider the following cases:

1.  $[G : H] \leq n$ .

After left-cleaning, there must be at least one entry of  $S'$  in  $H$ . So use Lemma 3.6 to left-extract entries of  $S'$  from  $H$  until *all* left cosets of  $H$  are full (this is possible since  $|S'| = n \geq [G : H]$ ). So the lemma is proved in this case.

2.  $[G : H] = n + 1$ .

If after left-cleaning we have at least one entry of  $S'$  in  $H$  then use Lemma 3.6 to left-extract entries of  $S'$  from  $H$  until  $H$  is empty, and thus all non-identity left cosets of  $H$  contain a primitive element (as there are only  $n$  of them). If after left-cleaning we instead have that no entry of  $S'$  lies in  $H$ , then all non-identity cosets of  $H$  contain primitive elements. Now we appeal to Theorem 5.5 to show that  $H$  itself must contain a primitive element, as  $[G : H] = n + 1 < n + 2^n$  (note that we cannot have  $G/H \cong C_2^n$  as  $n \geq 2$  and thus  $n + 1 < 2^n$ ).

3.  $[G : H] = n + 2$ .

Left-clean  $S$  to  $S'$ , then use Lemma 3.6 to left-extract entries of  $S'$  from  $H$  until  $H$  is empty. So we need only consider the case where we have a generating  $n$ -tuple  $S''$  where  $H$  and  $xH$  are empty for some  $x \notin H$ . By Lemma 5.8,  $xH$  must contain a primitive element. By Theorem 5.5, apart from the case  $n = 2$  and  $G/H \cong C_2^2$  (whereupon  $H = [G, G]G^2$ ),  $H$  must contain a primitive element (it is only in this exceptional case that  $n + 2 \geq |C_2^n|$ ).  $\square$

Our analysis of the possible location of primitive elements, relative to cosets of  $H < F_n$ , was motivated by the following result of Parzanchevski and Puder in [16]:

**Theorem 5.10** ([16, Corollary 1.3]). *The set  $P$  of primitive elements in  $F_n$  is closed in the profinite topology.*

**Corollary 5.11.** *Given  $F_n$ , and  $w \in F_n$  a non-primitive element, there is a finite index subgroup  $H < F_n$  such that the coset  $wH$  does not contain any primitive elements (but of course contains  $w$ ). Taking  $w = e$  gives a finite index subgroup with no primitive elements.*

Given that the above result is existential, we decided to apply our techniques to look for explicit examples of subgroups with no primitive elements; Theorems 5.4 and 5.5 came about from this analysis, somewhat serendipitously.

We finish by remarking that a recent result of Clifford and Goldstein in [6] proves there is an algorithm to determine whether or not a finitely generated subgroup of  $F_n$  contains a primitive element, although they say that they do not expect it to be implemented in practice. One of our overall aims is to give a characterisation of such subgroups that leads to computationally-efficient recognition.

## REFERENCES

- [1] A. Blass, *Injectivity, Projectivity, and the Axiom of Choice*, Trans. Amer. Math. Soc. **255**, 31–59, (1979).
- [2] J. Button, M. Chiodo, M. Zeron-Medina Laris, *Coset intersection graphs, and transversals as generating sets for finitely generated groups*, “Research Perspectives CRM Barcelona”, Trends in Mathematics, Vol. 1, Birkhäuser, *To appear*.
- [3] J. Button, M. Chiodo, M. Zeron-Medina Laris, *Coset intersection graphs for groups*, American Mathematical Monthly, *To appear* (preprint at arXiv:1304.6111v1).
- [4] P. Cameron, *Generating a group by a transversal* <http://www.maths.qmul.ac.uk/~pjc/papers.html>
- [5] P. Cameron, <http://www.maths.qmul.ac.uk/~pjc/oldprob.html>
- [6] A. Clifford and R. Goldstein, *Subgroups of free groups and primitive elements*, J. Group Theory **13**, 601–611, (2010).
- [7] H. S. M. Coxeter, J. A. Todd, *A practical method for enumerating cosets of a finite abstract group*, Proceedings of the Edinburgh Mathematical Society, Series II, **5**, 26–34 (1936).
- [8] M. Dunwoody, *Nielsen transformations*, 1970 Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967), 45–46, Pergamon, Oxford.
- [9] M. J. Evans, *Primitive elements in free groups*, Proc. Amer. Math. Soc. **106**, 313–316, (1989).
- [10] I. Kapovich, A. Myasnikov, *Stallings foldings and subgroups of free groups*, J. Algebra. **248**, 608–668, (2002).
- [11] R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*. Springer-Verlag, Berlin-Heidelberg-New York 1977.
- [12] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Mathematics **212**, Birkhäuser Verlag, Basel, (2003).
- [13] C. F. Miller III, *Decision problems for groups-survey and reflections*. Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989), Math. Sci. Res. Inst. Publ., **23**, Springer, New York, 1–59 (1992).
- [14] G. A. Noskov, *Primitive elements in a free group*, Matematicheskii Zametki **30**, 497–500, (1981).
- [15] I. Pak, *What do we know about the product replacement algorithm?*, Groups and computation, III, 301–347, Ohio State Univ. Math. Res. Inst. Publ. **8**, de Gruyter, Berlin, (2001).
- [16] O. Parzanchevski, D. Puder, *Measure preserving words are primitive*, arXiv:1202.3269v1 (2012).
- [17] J. Whiston, *Maximal independent generating sets of the symmetric group*, J. Algebra **232**, 255–268, (2000).

SELWYN COLLEGE, CAMBRIDGE  
 GRANGE ROAD, CAMBRIDGE, CB3 9DQ, UK  
 J.O.BUTTON@DPMMS.CAM.AC.UK

MATHEMATICS DEPARTMENT, UNIVERSITY OF NEUCHÂTEL  
 RUE EMILE-ARGAND 11, NEUCHÂTEL, CH-2000, SWITZERLAND  
 MAURICE.CHIODO@UNINE.CH

31 MARINER'S WAY, CAMBRIDGE, CB4 1BN, UK  
 MARIANOZERON@GMAIL.COM